UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Christopher Morbitzer and Briann Morbitzer, Plaintiffs, v. John Doe, Defendant.	Case No. 21-cv-2038 (PJS/HB) **ORDER**

HILDY BOWBEER, United States Magistrate Judge

This matter is before the Court on Plaintiffs' Motion for Leave to Take Discovery Prior to Rule 26(f) Conference (Mot. Leave Serve Subpoena [ECF No. 5]), to allow them to serve subpoenas on Cellco Partnership d/b/a Verizon Wireless and Charter Communications d/b/a Spectrum. The motion is granted, as set forth below.

I. Background

On September 15, 2021, the Morbitzers filed this case against a John Doe Defendant in the District of Minnesota. (Compl. [ECF No. 1].) They allege Doe violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2021).

According to the Complaint, Briann Morbitzer recently changed her phone number, giving up her previous number, and Doe subsequently came into possession of that number. (Compl. ¶¶ 11-12.) Doe requested and received a password reset confirmation sent to Briann's old phone number, which allowed Doe to reset the

passwords on and seize control of the plaintiffs' email and social media accounts. (Compl. ¶¶ 13-14.) Doe leveraged that access to view and download their financial, credit, tax, and business records from a secure online storage system, make unauthorized purchases and money transfers, and open an account in Briann's name on a cryptocurrency exchange. (Compl. ¶¶ 13-18, 20.) The Morbitzers have since regained control of all accounts except Briann's email and cloud storage account used to communicate with patients and store records for her speech therapy business. (Compl. ¶ 20.) Doe retains control of that account. (*Id.*)

The Morbitzers represent that they have taken reasonable steps to identify Doe, including calling the phone number used to change the passwords, and identifying the two IPv6 addresses and smart phone models from which the unauthorized account accesses and password changes originated, as well as the internet service providers and approximate geographic location of those IP addresses. (Mem. Supp. Mot. Leave Serve Subpoena ¶¶ 2, 4-6, 10-11 [ECF No. 6].) They also searched public information for the identity of the person associated with the addresses and phone number. (*Id.* ¶ 10.)

They identified Verizon Wireless and Charter Communications as the providers to which the two addresses are assigned. (*Id.* ¶ 6.) They also identified a city near which the accesses originated within the 320 area code. (*Id.* ¶ 9.) They could not identify the person using those addresses or phone number. (*Id.* ¶¶ 10-11.)

The Morbitzers seek the identity of the person who now possesses Briann's old phone number, alleging that person must be Doe. (*Id.*) This allegation is based on the circumstances that the old number had a 320 area code and was carried by Verizon

Wireless, matching the area code and carrier from which the unauthorized accesses occurred. (*Id.*) Furthermore, the first password change (which enabled the subsequent password changes) could only have been accomplished using a confirmation link sent to the old phone number, suggesting that Doe used that number to accomplish the password change. (*Id.*) Taken together, this suggests that Doe accessed the Morbitzers' accounts from the IP addresses to assigned Verizon Wireless and Charter Communication in the 320 area code, and requested password resets for those accounts by using Briann Morbitzer's old 320 area code phone number carried by Verizon Wireless.

The Morbitzers contend that they can learn the identity of Doe by subpoenaing Verizon Wireless and Charter Communications for the true name and physical address of the subscriber(s) associated with the phone number and IP addresses. (*Id.* ¶ 14.) They also contend that time is of the essence because these providers store that subscriber information for only a limited time once an account deactivates, so delaying the subpoena risks the loss of that information. (*Id.* ¶¶ 12-13, 15.) Finally, they commit to using that information solely to establish this Court's personal jurisdiction over Doe, serve process on Doe, and prosecute their claim against Doe. (*Id.* ¶ 14.)

II. Discussion

A. Relevant Legal Standards and Case Authority

Rule 26(d) of the Federal Rules of Civil Procedure prohibits a party from "seek[ing] discovery from any source before the parties have conferred as required by Rule 26(f), except . . . when authorized by these rules, by stipulation, or by court order." Fed. R. Civ. P. 26(d)(1). The Morbitzers are in a Catch-22 where they cannot identify

Doe so they cannot hold the Rule 26(f) conference, which is a prerequisite to accessing the discovery tools through which they could learn Doe's identity. They argue that they can obtain Doe's identity from Verizon Wireless and Charter Communications, which are likely to have Doe's contact information. (Mem. Supp. Mot. Leave Serve Subpoena ¶ 14.)

Although the United States Court of Appeals for the Eighth Circuit has not adopted a standard to govern when a court should permit expedited discovery, this Court generally applies a "good cause" standard. *Let Them Play MN v. Walz*, 517 F. Supp. 3d 870, 889 (D. Minn. 2021); *ALARIS Grp., Inc. v. Disability Mgmt. Network, Ltd.*, No. CV 12-446 (RHK/LIB), 2012 WL 13029504, at *2 (D. Minn. May 30, 2012). Other courts within the circuit use a similar standard. *See, e.g.*, *Wachovia Sec., L.L.C. v. Stanton*, 571 F. Supp. 2d 1014, 1050 (N.D. Iowa 2008). The party seeking the early discovery must show "good cause—i.e., that the need for expedited discovery outweighs the prejudice to the responding party." *Let Them Play MN*, 517 F. Supp. 3d at 889 (quotation omitted).

To determine the appropriateness of early discovery, judges in this District have reviewed "(1) whether a preliminary injunction is pending; (2) the breadth of discovery requests; (3) the purpose for requesting the expedited discovery; (4) the burden on the defendants to comply with the requests; and (5) how far in advance of the typical discovery process the request was made." *Id.*; *Council on Am.-Islamic Rels.–Minnesota v. Atlas Aegis, LLC*, 497 F. Supp. 3d 371, 380 (D. Minn. 2020). Judges in this District have also considered a set of factors articulated by the United States Court of Appeals for the Second Circuit: (1) whether the plaintiff demonstrates a prima facie claim of

actionable harm; (2) the specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) the need for the subpoenaed information to advance the claim, and (5) the objecting party's expectation of privacy. *Paisley Park Enterprises, Inc. v. Ziani*, No. 18-CV-2556 (DSD/TNL), 2018 WL 6567828, at *3 (D. Minn. Dec. 13, 2018) (citing *Arista Recs., LLC v. Doe 3*, 604 F.3d 110, 123 (2d Cir. 2010)); *Strike 3 Holdings, LLC v. Doe*, No. 18-CV-0778 (PJS/HB), 2018 WL 2278111, at *3 (D. Minn. May 18, 2018).

This Court is also guided by the Eighth Circuit's reasoning recognizing the important role an internet service provider may play in helping a plaintiff identify a defendant anonymized behind an IP address. "Only the ISP . . . can link a particular IP address with an individual's name and physical address." *In re Charter Commc'ns, Inc., Subpoena Enf't Matter*, 393 F.3d 771, 774 (8th Cir. 2005). In the same case, the Eighth Circuit endorsed in dicta the sort of procedure Plaintiffs seek here, but in the context of copyright infringement claims:

> [A]s a practical matter, copyright owners cannot deter unlawful peer-to-peer file transfers unless they can learn the identities of persons engaged in that activity. However, [copyright owners] can . . . file a John Doe suit, along with a motion for third-party discovery of the identity of the otherwise anonymous "John Doe" defendant.

Id. n.3. With this guidance in mind, the Court concludes that both sets of factors support good cause here.

B. *Let Them Play MN* Factors

This Court concludes that the factors identified in *Let Them Play MN* support good cause. 517 F. Supp. 3d at 889. First, the Morbitzers complaint requests relief, in part, as a preliminary injunction against Doe to prevent Doe from accessing Plaintiffs' accounts and protected information, interfering with Plaintiffs' business operations and medical treatment, and retaining possession of or trafficking any document or information obtained through the unauthorized accesses. (Compl. at 13.) Though the Morbitzers have not moved for the preliminary injunction, all indications at this early stage of the case are that they intend to do so once they can identify the Doe Defendant. Second, their discovery request is limited, seeking only the name and physical address of the subscribers assigned to two IP addresses and a single phone number at the time of the violations, who they believe is a single individual. (Mem. Supp. Mot. Leave Serve Subpoena ¶¶ 2, 4-6, 10-11.) *See Council on Am.-Islamic Rels –Minnesota*, 497 F. Supp. 3d at 380 (describing as narrow a request for the same information on ten individuals). Third, the discovery is necessary for the Morbitzers to properly identify the defendant, serve him or her, and advance the claim against that individual. Fourth, the defendant Doe will not be burdened by this request, and the burden on the third-party ISPs is minimal due to the narrow nature of the request and the small amount of information sought. Finally, as in *Council on Am.-Islamic Rels.–Minnesota*, "although the request is made [well] in advance of the usual discovery process, this is not enough to overcome the other factors." *Id.*

C. Second Circuit Factors

The Second Circuit factors likewise support good cause. First, the Morbitzers amply demonstrate a prima facie claim of actionable harm under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The Act protects "protected computers," which includes computers "used in or affecting interstate or foreign commerce or communication," by forbidding a wide array of behavior. *Id.* (e)(2)(B). The following are all violations of the Act: "intentionally access[ing] a computer without authorization . . . and thereby obtain[ing] . . . information from any protected computer," "knowingly and with intent to defraud, access[ing] a protected computer without authorization . . . and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value," "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or . . . caus[ing] damage and loss," and "knowingly and with intent to defraud traffic[king] . . . in any password or similar information through which a computer may be accessed without authorization, if such trafficking affects interstate or foreign commerce." *Id.* (a)(2)(C), (a)(4), (a)(5)(B)–(C), (a)(6)(A). The Act permits "any person who suffers damage or loss by reason of a violation . . . [to] maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief," so long as the violation caused at least $5,000 of loss during a 1-year period, or "the modification or impairment, or potential modification or impairment, of [] medical examination, diagnosis, treatment, or care of [an individual]," or "physical injury to any person", or "a threat to public health and safety." *Id.* (c)(4)(A)(i)(I)–(IV), (g).

The Morbitzers allege Doe intentionally and without authorization accessed protected computer systems to obtain their financial, credit, tax, and business records, including records about Briann's out-of-state patients for her speech therapy business, and used that information to attempt unauthorized purchases and money transfers, and open a fraudulent account in Briann's name on a cryptocurrency exchange. (Compl. ¶¶ 26-33.) They argue Doe's actions violated each prohibition from subpart (a) listed above. *(Id.*) They claim losses in excess of $5,000 from investigating and responding to Doe's actions and the monetary impacts of Doe's actions to their finances and businesses, plus impairment to the care Briann offers to her patients up to and including personal injury to those patients, and finally a threat to public health. (*Id.* ¶¶ 34-37.) They finally claim a variety of economic and non-economic damages. (*Id.* ¶ 38.) This easily satisfies the first factor.

The second, third, and fourth factors were addressed by the *Let Them Play MN* discussion above. In brief, the request is limited to only the subscriber's name and physical address, the information cannot be obtained through any publicly available source based on the Morbitzers' current knowledge of the subscriber but Verizon Wireless and Charter Communication likely have it in discoverable form, and the information is necessary to advance the Morbitzers' case. *See, e.g.*, *Strike 3 Holdings, LLC*, 2018 WL 2278111, at *4-5 (D. Minn. May 18, 2018).

The final factor, the subscriber's expectation of privacy in their name and address, "is outweighed by [Plaintiffs'] right to use the judicial process to pursue a plausible claim . . . , especially given that the Court can craft a limited protective order pursuant to

Federal Rule of Civil Procedure 26(c) to protect an innocent ISP subscriber." *Id.* at *5. Specifically, judges in this District have concluded in the past that a subscriber has minimal Fourth Amendment-protected privacy in their contact information disclosed to an internet service provider, and that minimal privacy interest does not overcome the plaintiff's right to learn that information to pursue a claim against the subscriber provided good cause has been shown. *See*, *e.g.*, *Strike 3 Holdings, LLC v. Doe*, 337 F. Supp. 3d 246, 256 (W.D.N.Y. 2018); *Strike 3 Holdings, LLC*, *v. Doe*, No. CV 18-774 (DWF/DTS), 2018 WL 4210202, at *2 (D. Minn. Sept. 4, 2018); *Strike 3 Holdings, LLC*, 2018 WL 2278111, *5 (D. Minn. May 18, 2018).

The Morbitzers identify a concern that Verizon Wireless and Charter Communication may be "cable operators" within the meaning of the Communications Act, 47 U.S.C. § 522(5) (2021). (Mem. Supp. Mot. Leave Serve Subpoena ¶ 26.) If so, the Act forbids them from disclosing "personally identifiable information concerning any subscriber without the prior . . . consent of the subscriber." *Id.* § 551(c)(1) (2021). But an operator may disclose the information "pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed." *Id.* (2)(B) (2021). If Verizon Wireless or Charter Communication is a "cable operator" under the Act, this Court authorizes them to disclose subscriber information under 47 U.S.C. § 551(2)(B) to the extent necessary to obtain the information described in this order. Verizon Wireless and Charter Communication shall comply with any applicable notification requirements.

The Court also acknowledges that Doe, the subscriber, may not have been the actual violator. The actual violator could be anyone with access to the subscriber's internet connection and Briann's phone number. This risk can be adequately managed through the litigation process. In addition, the Court will limit the Morbitzers' use of the information to only those uses that they have indicated in their motion and this Court has found acceptable.

Accordingly, **IT IS HEREBY ORDERED** that Plaintiffs Christopher Morbitzer and Briann Morbitzer's Motion for Leave to Take Discovery Prior to a Rule 26(f) Conference [ECF No. 5] is **GRANTED** as follows:

1. Plaintiffs may immediately serve one subpoena on each of Doe's ISPs, Verizon Wireless and Charter Communication, pursuant to Federal Rule of Civil Procedure 45. The subpoenas must be limited to one category of documents identifying the particular subscriber(s) in the Motion. The subpoena must be limited to only information reasonably calculated to ascertain the identity of the John Doe Defendant(s) assigned to the IP addresses and phone number identified in the Motion during the time period(s) of the alleged violating activity referenced in the Motion. Plaintiff must serve a copy of this Order together with each subpoena.

2. Verizon and Charter are authorized to disclose the subscriber information in compliance with 47 U.S.C. § 551(2)(B) insofar as that Act may apply.

3. Plaintiff may use any information produced by Verizon or Charter in response to the subpoena only for the purpose of protecting and enforcing Plaintiff's rights as set forth in its Complaint and for no other purpose. This limitation on the use of the information will not expire absent further order of the Court.

4. No other discovery is authorized at this time.

Dated: September 21, 2021

s/ Hildy Bowbeer
HILDY BOWBEER
United States Magistrate Judge